

Day 2

Miles Smid
NIST

TV0FISH
SEPPENT
SAFEPT
BUNDAEL
PCG
MAGENTA
MAGENTA
LOH197
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256
TV0FISH
SEPPENT
SAFEPT
BUNDAEL
PCG
MAGENTA
MAGENTA
LOH197
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256

TVORISH
SERPENT
SAFEH
BUNDAEL
PCG
MARS
MAGENTA
LOH97
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256
TVORISH
SERPENT
SAFEH
BUNDAEL
PCG
MARS
MAGENTA
LOH97
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256



Second AES Conference?

AES

Second AES Candidate Conference

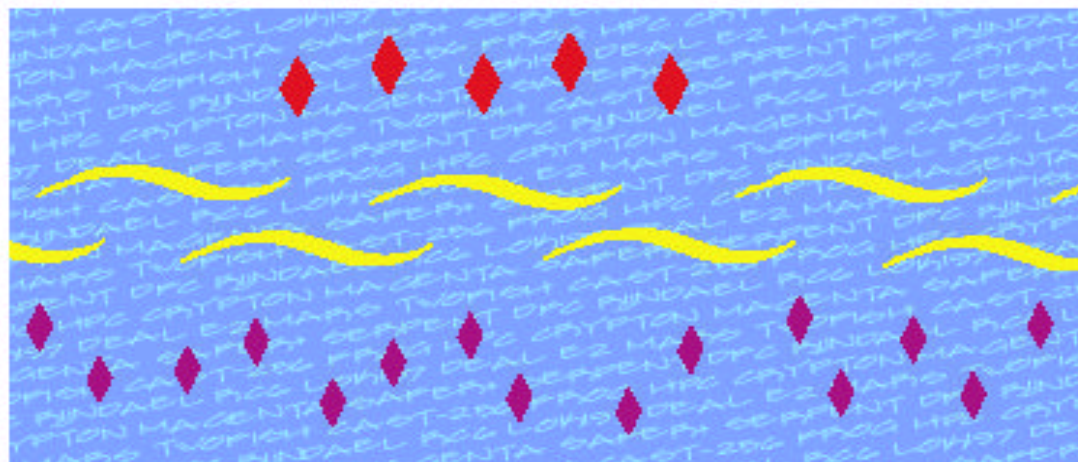
Rome, Italy

March 22-23,
1999

TV0FISH
SEPPENT
SAFEAT
BUNDAEL
PCC
MARS
MAGENTA
LOH97
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256
TV0FISH
SEPPENT
SAFEAT
BUNDAEL
PCC
MARS
MAGENTA
LOH97
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256

AES

A Crypto Algorithm for the Twenty-first Century . . .



THE SECOND
ADVANCED ENCRYPTION STANDARD
CANDIDATE CONFERENCE

MARCH 22-23, 1999

HOTEL QUIRINALE
ROME, ITALY

SPONSORED BY:
INFORMATION TECHNOLOGY LABORATORY
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

TRIVIAL
SERPENT
SAFER
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256
TRIVIAL
SERPENT
SAFER
BLINDAEL
RC6
MARS
MAGENTA
LOH197
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256

TVOFISH
SERPENT
SAFER+
BUNDAEL
PCG
MARS
MAGENTA
LOH97
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256
TVOFISH
SERPENT
SAFER+
BUNDAEL
PCG
MARS
MAGENTA
LOH97
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256

Thanks to Raif Naffah
and the

CRYPTIX

Development Team



Issues/Questions



TWOPIST
SEPPENT
SAFEPI
BUNDAEL
PCC
MAGENTA
MAGENTA
LOH197
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256
TWOPIST
SEPPENT
SAFEPI
BUNDAEL
PCC
MAGENTA
MAGENTA
LOH197
HPC
PROG
E2
DPC
DEAL
CRYPTON
CAST-256